Available online at www.sciencedirect.com
SCIENCE DIRECT®
Discrete Applied Mathematics 128 (2003) 305–316
DISCRETE APPLIED MATHEMATICS
www.elsevier.com/locate/dam

Some constacyclic codes over Z_{2^k} and binary quasi-cyclic codes

H. Tapia-Recillas[a,*,1], G. Vega[b]

[a] *Departamento de Matemáticas, Universidad Autónoma Metropolitana-Iztapalapa, 09340 México, DF, Mexico*

[b] *Dirección General de Servicios de Cómputo Académico, Universidad Nacional Autónoma de México, 04510 México, DF, Mexico*

Received 27 February 2001; received in revised form 28 September 2001; accepted 8 April 2002

Abstract

The concept of negacyclic code was recently introduced in Wolfmann (IEEE Trans. Inform. Theory 45 (1999) 2527–2532), in which some relations between the negacyclic codes and their Gray map images are proved. In this note, for $k \geqslant 1$ an isometry φ^k between codes over $\mathbb{Z}_{2^{k+1}}$ and codes over $\mathbb{Z}_4$ is introduced and used to give a generalization of the Gray map equivalent to the one given in Carlet (IEEE Trans. Inform. Theory 44 (1998) 1543–1547). Furthermore, by means of this isometry, the concept of negacyclic codes is extended to codes over the ring $\mathbb{Z}_{2^{k+1}}$, obtaining a class of constacyclic codes referred to as *hpo-cyclic codes* (half plus one-cyclic codes). A characterization of these codes in terms of their images under φ^k is given. It is also proved that the generalized Gray map image of an *hpo*-cyclic code is a binary distance invariant (not necessarily linear) quasi-cyclic code. Finally, some linear *hpo*-cyclic codes are discussed and a few examples are given.

Keywords: Gray map; *Hpo*-cyclic; Negacyclic; Constacyclic; Quasi-cyclic and cyclic codes over $\mathbb{Z}_{2^k}$

1. Introduction

Let R be a commutative ring with identity and let n be a positive integer. For some fixed unit λ of R, let v_λ be the automorphism on R^n given by

$$v_\lambda(a_0, a_1, \ldots, a_{n-1}) = (\lambda a_{n-1}, a_0, a_1, \ldots, a_{n-2}).$$

* Corresponding author.
E-mail addresses: htr@xanum.uam.mx (H. Tapia-Recillas), gerardov@servidor.unam.mx (G. Vega).
[1] Partially supported by SNI-SEP and CONACyT, México.

0166-218X/03/$ - see front matter © 2003 Elsevier Science B.V. All rights reserved.
PII: S0166-218X(02)00453-5

Recall that a subset C of R^n is a *constacyclic* code of length n if there exists a unit λ of R such that it is invariant under the automorphism v_λ, that is, $v_\lambda(C) = C$. If $\lambda = 1$ the code is said to be cyclic.

Constacyclic linear codes of length n over R can be identified as ideals in the quotient ring $R[x]/(x^n - \lambda)$ via the isomorphism from R^n to $R[x]/(x^n - \lambda)$ defined by

$$(a_0, a_1, \ldots, a_{n-1}) \mapsto a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}. \tag{1}$$

In the following we will restrict the ring R to $\mathbb{Z}_{2^{k+1}}$, the ring of integers modulo 2^{k+1}, where k is a positive integer. For the special case $\lambda = -1$ and $k = 1$, the *negashift* map, v, over the ring $\mathbb{Z}_4$ of integers modulo 4 is introduced in [12] as the permutation on the module $\mathbb{Z}_4^n$, given as

$$v(a_0, a_1, \ldots, a_{n-1}) = (-a_{n-1}, a_0, a_1, \ldots, a_{n-2})$$

and a *negacyclic code* of length n over $\mathbb{Z}_4$ is defined as a subset C of $\mathbb{Z}_4^n$ such that $v(C) = C$.

For any positive integer k, if the unit λ in $\mathbb{Z}_{2^{k+1}}$ is equal to $2^k + 1$ (half of 2^{k+1} plus one), then a subset $C \subseteq \mathbb{Z}_{2^{k+1}}^n$ such that $v_\lambda(C) = C$ will be called an *hpo-cyclic code*.

For $k \geqslant 1$, an isometry φ^k between codes over $\mathbb{Z}_{2^{k+1}}$ and codes over $\mathbb{Z}_4$ is defined and used, together with the usual Gray map (i.e., on the ring $\mathbb{Z}_4$), to give an equivalent generalization of the Gray map, as introduced in [3]. A characterization of the *hpo*-cyclic codes in terms of their images under the isometry φ^k is given. It is also shown that the generalized Gray map image of an *hpo*-cyclic code of length n is a binary distance invariant (not necessarily linear) quasi-cyclic code, of length $2^k n$. Finally, some linear *hpo*-cyclic codes are discussed and a few examples are given.

2. Definitions, notation and preliminaries

Let $\mathbb{F}_2$ be the binary field, and for a positive integer n let $\mathbb{F}_2^n$ be the vector space of all binary vectors of length n. For any positive integer k let $\mathbb{Z}_{2^{k+1}}$ be the ring of integers modulo 2^{k+1}, and let $\mathbb{Z}_{2^{k+1}}^n$ be the module of all n-tuples with entries in $\mathbb{Z}_{2^{k+1}}$. For clarity, addition in $\mathbb{F}_2$, $\mathbb{F}_2[x]$ and $\mathbb{F}_2^n$ will be denoted by "$\oplus$", while addition in $\mathbb{Z}_{2^{k+1}}$, $\mathbb{Z}_{2^{k+1}}[x]$ and $\mathbb{Z}_{2^{k+1}}^n$ will be denoted by "$+$".

Let σ be the usual *shift* on $\mathbb{F}_2^{2n}$ and $\mathbb{Z}_{2^{k+1}}^n$. For any positive integer s, let $\mathscr{S}_s$ be the *quasi-shift* on $(\mathbb{F}_2^{2n})^s$ and $\mathscr{N}_s$ be the *quasi-negashift* on $(\mathbb{Z}_4^n)^s$ given by

$$\mathscr{S}_s(\tilde{a}^{(1)}|\tilde{a}^{(2)}|\ldots|\tilde{a}^{(s)}) = \sigma(\tilde{a}^{(1)})|\sigma(\tilde{a}^{(2)})|\ldots|\sigma(\tilde{a}^{(s)}),$$

$$\mathscr{N}_s(a^{(1)}|a^{(2)}|\ldots|a^{(s)}) = v(a^{(1)})|v(a^{(2)})|\ldots|v(a^{(s)}),$$

where "|" denotes the usual vector concatenation and $\tilde{a}^{(i)} \in \mathbb{F}_2^{2n}$, $a^{(i)} \in \mathbb{Z}_4^n$, for $i = 1, \ldots, s$.

A *cyclic* code of length $2n$ (respectively n) over $\mathbb{F}_2$ (respect. $\mathbb{Z}_{2^{k+1}}$), is a subset C of $\mathbb{F}_2^{2n}$ (respect. $\mathbb{Z}_{2^{k+1}}^n$) such that $\sigma(C) = C$. A *quasi-cyclic* code of order s and length $2ns$ over $\mathbb{F}_2$ is a subset C of $(\mathbb{F}_2^{2n})^s$ such that $\mathscr{S}_s(C) = C$. Equivalently, a

quasi-negacyclic code of order s and length ns over $\mathbb{Z}_4$ is a subset C of $(\mathbb{Z}_4^n)^s$ such that $\mathcal{N}_s(C) = C$. Clearly, when $s = 1$, the concepts of cyclic (respect. negacyclic) and quasi-cyclic (respect. quasi-negacyclic) codes are the same.

We now recall the definition of the *Gray map*, ϕ, from $\mathbb{Z}_4^n$ into $\mathbb{F}_2^{2n}$ as given in [5,12]: for any $Z = (z_1, z_2, \ldots, z_n) \in \mathbb{Z}_4^n$,

$$\phi(Z) = (r_1(z_1), \ldots, r_1(z_n), r_1(z_1) \oplus r_0(z_1), \ldots, r_1(z_n) \oplus r_0(z_n)),$$

where r_1 and r_0 are two mappings from $\mathbb{Z}_4$ into $\mathbb{F}_2$ such that, if $z \in \mathbb{Z}_4$ then the 2-adic expansion of z is $z = r_0(z) + 2r_1(z)$. Similarly, for $k \geqslant 1$, $k+1$ mappings r_i, $i = 0, 1, \ldots, k$, from $\mathbb{Z}_{2^{k+1}}$ into $\mathbb{F}_2$ are introduced in such a way that if $a \in \mathbb{Z}_{2^{k+1}}$, the 2-adic expansion of a is $a = r_0(a) + 2r_1(a) + \cdots + 2^k r_k(a)$. Using the 2-adic expansion of any element in $\mathbb{Z}_{2^{k+1}}$, the operation "$\odot$" on $\mathbb{Z}_{2^{k+1}}$ is introduced as follows: if $a, b \in \mathbb{Z}_{2^{k+1}}$, then

$$a \odot b = (r_0(a)r_0(b)) + 2(r_1(a)r_1(b)) + \cdots + 2^k(r_k(a)r_k(b)).$$

This operation is extended to $\mathbb{Z}_{2^{k+1}}^n$ in the following natural way: if $A = (a_0, \ldots, a_{n-1})$, $B = (b_0, \ldots, b_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$ then define $A \odot B = (a_0 \odot b_0, \ldots, a_{n-1} \odot b_{n-1})$.

For $k \geqslant 2$, define $\rho_k : \mathbb{Z}_{2^{k+1}} \to \mathbb{F}_2^{k-1}$ as $\rho_k(a) = (r_{k-1}(a), \ldots, r_2(a), r_1(a))$. For all $i \in \{0, 1, \ldots, 2^{k-1} - 1\}$, let $\alpha_i^k \in \mathbb{F}_2^{k-1}$ be the binary expression of i using $k-1$ bits, where the most significant bit is on the left, e.g. if $k = 5$ and $i = 13$ then $\alpha_{13}^5 = (1101)$. By means of ρ_k and α_i^k, the following functions $\varphi_i^k : \mathbb{Z}_{2^{k+1}} \to \mathbb{Z}_4$ are introduced:

$$\varphi_i^k(a) = 2(r_k(a) \oplus (\rho_k(a) \cdot \alpha_i^k)) + r_0(a), \quad \forall i = 0, 1, \ldots, 2^{k-1} - 1, \tag{2}$$

where "$\cdot$" denotes the usual dot product in $\mathbb{F}_2^{k-1}$. The action of the functions φ_i^k are extended to $\mathbb{Z}_{2^{k+1}}^n$ as follows: if $A = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{Z}_{2^{k+1}}^n$ then $\varphi_i^k(A) = (\varphi_i^k(a_0), \varphi_i^k(a_1), \ldots, \varphi_i^k(a_{n-1}))$. Thus, the map $\varphi^k : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{Z}_4^{2^{k-1}n}$ is introduced

$$\varphi^k(A) = (\varphi_0^k(A), \varphi_1^k(A), \ldots, \varphi_{2^{k-1}-1}^k(A)), \quad \forall A \in \mathbb{Z}_{2^{k+1}}^n.$$

For completeness, $\varphi^1 : \mathbb{Z}_4^n \to \mathbb{Z}_4^n$ is defined as the identity map, that is $\varphi^1(A) = A$. Using the map φ^k, an equivalent definition of the *generalized Gray map* $\Phi : \mathbb{Z}_{2^{k+1}}^n \to \mathbb{F}_2^{2^k n}$, as introduced in [3], can be given

$$\Phi(A) = (\phi\varphi_0^k(A), \phi\varphi_1^k(A), \ldots, \phi\varphi_{2^{k-1}-1}^k(A)), \quad \forall A \in \mathbb{Z}_{2^{k+1}}^n. \tag{3}$$

Remark 1. An alternative way to define the generalized Gray map is $\Phi(A) = \phi\varphi^k(A)$. The main difference between this definition and the one given by Eq. (3) is the way in which the bits of the image of the generalized Gray map are listed. In either case, it must be observed that Φ and φ^k are both injective mappings.

The *Lee weight*, wt_L, of $0, 1, 2, 3 \in \mathbb{Z}_4$ is $0, 1, 2, 1$, respectively, and the Lee weight $wt_L(A)$ of $A \in \mathbb{Z}_4^n$ is the rational sum of the Lee weights of its components. The *Lee distance*, d_L, is defined as $d_L(A, B) = wt_L(A - B)$ for all $A, B \in \mathbb{Z}_4^n$. For $k \geqslant 1$, the

homogeneous weight, wt_{hom}, on $\mathbb{Z}_{2^{k+1}}$ is defined as (see [4,6]):

$$wt_{\mathrm{hom}}(a) = \begin{cases} 0 & \text{if } a = 0, \\ 2^k & \text{if } a = 2^k, \\ 2^{k-1} & \text{otherwise,} \end{cases} \qquad \forall a \in \mathbb{Z}_{2^{k+1}}.$$

Again, for $A \in \mathbb{Z}_{2^{k+1}}^n$, the value $wt_{\mathrm{hom}}(A)$ is taken as the rational sum of the homogeneous weights of its components, and the *homogeneous metric*, δ_{hom}, is given by $\delta_{\mathrm{hom}}(A,B) = wt_{\mathrm{hom}}(A-B)$ for all $A,B \in \mathbb{Z}_{2^{k+1}}^n$.

For $n = 1$, $k \geqslant 2$, and for $a \in \mathbb{Z}_{2^{k+1}}$, the function $f(i) = r_k(a) \oplus (\rho_k(a) \cdot \alpha_i^k)$ in Eq. (2) is an affine Boolean function in $k-1$ variables. Hence, the vector $\varphi^k(a) = (\varphi_0^k(a), \varphi_1^k(a), \ldots, \varphi_{2^{k-1}-1}^k(a))$ has one of the following forms:

- the null vector if $a = 0$,
- all of its entries are equal to 2 if $a = 2^k$,
- half of its entries are equal to 2 and the other half are equal to 0 if a is an even number different from 0 and 2^k,
- all of its entries have the value 1 or 3 if a is odd.

The conclusion is, in any case, that $wt_{\mathrm{hom}}(a) = wt_{\mathrm{L}}(\varphi^k(a))$. Thus, we have proved the following:

Proposition 2. *The map φ^k is an isometry from $(\mathbb{Z}_{2^{k+1}}^n, \delta_{\mathrm{hom}})$ into $(\mathbb{Z}_4^{2^{k-1}n}, d_{\mathrm{L}})$.*

In [5], the authors take the usual binary Hamming distance, d_{H}, on $\mathbb{F}_2^{2n}$ in order to prove that the Gray map, ϕ, from $\mathbb{Z}_4^n$ into $\mathbb{F}_2^{2n}$ is an isometry. As a consequence of the previous Proposition we have, as in [3], the following:

Corollary 3. *The generalized Gray map, Φ, is an isometry from $(\mathbb{Z}_{2^{k+1}}^n, \delta_{\mathrm{hom}})$ into $(\mathbb{F}_2^{2^k n}, d_{\mathrm{H}})$.*

The isometry φ^k is studied more extensively in [11] and the following properties will be useful later.

Proposition 4. *Let $A, B \in \mathbb{Z}_{2^{k+1}}^n$, where $A = (a_0, \ldots, a_{n-1})$, then*

$$\varphi^k(2^k A + B) = \bar{1} \otimes 2\bar{r}_0(A) + \varphi^k(B),$$

where $\bar{1}$ is the all one vector of length 2^{k-1}, "$\otimes$" is the Kronecker product [8, chapter 14, p. 421] *and $\bar{r}_0(A)$ is a binary vector of length n that has a one in its i-th entry if and only if a_{i-1} is odd, for $i = 1, \ldots, n$.*

Theorem 5. *Let C be a linear code over $\mathbb{Z}_{2^{k+1}}$, then for $k > 1$ the following properties are equivalent.*

(1) *$\varphi^k(C)$ is linear.*

(2) $\Phi(C)$ *is linear.*
(3) $2(A \odot B) \in C$ *for all* $A, B \in C$.

3. *Hpo*-cyclic, negacyclic and quasi-cyclic codes

In this section, a characterization of the *hpo*-cyclic codes in terms of their images under the isometry φ^k is given. A result similar to [12, Theorem 3.5] is also proved. The following two Propositions allow us to establish the connection between negacyclic and *hpo*-cyclic codes.

Proposition 6. *Let* r_i, $i=0,1,\ldots,k$, *be the mappings as defined above and let* $\lambda=2^k+1$ *be a unit of* $\mathbb{Z}_{2^{k+1}}$. *Then for all* $a \in \mathbb{Z}_{2^{k+1}}$:

$$r_i(\lambda a) = \begin{cases} r_i(a) & if\ \ i = 0,1,\ldots,k-1, \\ r_k(a) \oplus r_0(a) & if\ \ i = k. \end{cases}$$

Proof. $\lambda a = (2^k+1)(\sum_{i=0}^{k} 2^i r_i(a)) = \sum_{i=0}^{k-1} 2^i r_i(a) + 2^k(r_0(a) \oplus r_k(a))$. □

Proposition 7. *Let* φ_i^k, $i=0,1,\ldots,2^{k-1}-1$ *be the mappings as defined previously and let* $\lambda = 2^k + 1$. *Then for all* $a \in \mathbb{Z}_{2^{k+1}}$:

$$\varphi_i^k(\lambda a) = -\varphi_i^k(a). \tag{4}$$

Proof. The proof is an immediate consequence of the definition of the mappings φ_i^k in Eq. (2) and Proposition 6. □

The next result establishes a characterization of an *hpo*-cyclic code C in $\mathbb{Z}_{2^{k+1}}^n$ and its image under the map φ^k.

Theorem 8. *Let* C *be a code over* $\mathbb{Z}_{2^{k+1}}$ *of length* n. *Then* C *is an hpo-cyclic code if and only if* $\varphi^k(C)$ *is a quasi-negacyclic code of order* 2^{k-1} *and length* $2^{k-1}n$.

Proof. If $\lambda = 2^k + 1 \in \mathbb{Z}_{2^{k+1}}$, it follows from Proposition 7 that for all φ_i^k:

$$\varphi_i^k(v_\lambda(A)) = v(\varphi_i^k(A)), \quad \forall A \in \mathbb{Z}_{2^{k+1}}^n. \tag{5}$$

Thus $\varphi^k(v_\lambda(C)) = \mathcal{N}_{2^{k-1}}(\varphi^k(C))$ and the result follows from the fact that φ^k is an injective map. □

If in the previous Theorem $k = 1$, the concepts of an *hpo*-cyclic code and a negacyclic code are the same. Thus, this result shows that the *hpo*-cyclic codes are natural generalizations of the negacyclic codes as introduced in [12]. The following result is also proved in [12].

Proposition 9. *If v is the negashift on $\mathbb{Z}_4^n$, σ is the shift on $\mathbb{F}_2^{2n}$, and if ϕ is the Gray map from $\mathbb{Z}_4^n$ into $\mathbb{F}_2^{2n}$, then*

$$\phi v = \sigma\phi.$$

As a consequence of Eq. (5) and the previous proposition, a result similar to Proposition 9, is

Proposition 10. *If $\lambda = 2^k + 1 \in \mathbb{Z}_{2^{k+1}}$ then*

$$\Phi v_\lambda = \mathscr{S}_{2^{k-1}}\Phi. \tag{6}$$

Proof. Let $A \in \mathbb{Z}_{2^{k+1}}^n$, then

$$\begin{aligned}\Phi(v_\lambda(A)) &= (\phi\varphi_0^k(v_\lambda(A)), \phi\varphi_1^k(v_\lambda(A)), \ldots, \phi\varphi_{2^{k-1}-1}^k(v_\lambda(A)))\\ &= (\phi v\varphi_0^k(A), \phi v\varphi_1^k(A), \ldots, \phi v\varphi_{2^{k-1}-1}^k(A))\\ &= (\sigma\phi\varphi_0^k(A), \sigma\phi\varphi_1^k(A), \ldots, \sigma\phi\varphi_{2^{k-1}-1}^k(A)) = \mathscr{S}_{2^{k-1}}(\Phi(A)).\end{aligned}$$ □

The corresponding generalization of [12, Theorem 3.5] is as follows:

Theorem 11. *The generalized Gray map image of a linear hpo-cyclic code over $\mathbb{Z}_{2^{k+1}}$ of length n, is a binary-distance-invariant (not necessarily linear) quasi-cyclic code of order 2^{k-1} and length $2^k n$.*

Proof. Straightforward from Corollary 3, Theorem 8 and Eq. (6). □

4. Generalized gray images of *hpo*-cyclic codes of odd length

The main result of this section is the generalization of [12, Corollary 3.8].

Proposition 12. *Let n be an odd positive integer, $\lambda = 2^k + 1 \in \mathbb{Z}_{2^{k+1}}$ and let $\tilde{\mu}_\lambda$ be the permutation on $\mathbb{Z}_{2^{k+1}}^n$ given by*

$$\tilde{\mu}_\lambda(a_0, a_1, \ldots, a_i, \ldots, a_{n-1}) = (a_0, \lambda a_1, \ldots, \lambda^i a_i, \ldots, \lambda^{n-1} a_{n-1}).$$

Then $D \subseteq \mathbb{Z}_{2^{k+1}}^n$ is a linear cyclic code if and only if $\tilde{\mu}_\lambda(D)$ is a linear hpo-cyclic code.

Proof. Since λ is a unit of $\mathbb{Z}_{2^{k+1}}$ and $\tilde{\mu}_\lambda$ is $\mathbb{Z}_{2^{k+1}}$-linear, D is linear if and only if $\tilde{\mu}_\lambda(D)$ is also linear. Since n is odd and $\lambda^2 = 1$, then $\tilde{\mu}_\lambda(\lambda\sigma(A)) = v_\lambda(\tilde{\mu}_\lambda(A))$ for all $A \in D$. Thus, $\sigma(A) \in D \Leftrightarrow \lambda\sigma(A) \in D \Leftrightarrow \tilde{\mu}_\lambda(\lambda\sigma(A)) = v_\lambda(\tilde{\mu}_\lambda(A)) \in \tilde{\mu}_\lambda(D)$. □

Since $-1 = 3$ in $\mathbb{Z}_4$ and $\lambda^2 = 1$ in $\mathbb{Z}_{2^k+1}$, a relation between the function $\tilde{\mu}_\lambda$ and the functions φ_i^k, equivalent to that given by Eq. (5), is

$$\varphi_i^k(\tilde{\mu}_\lambda(A)) = \tilde{\mu}_3(\varphi_i^k(A)), \quad \forall A \in \mathbb{Z}_{2^{k+1}}^n. \tag{7}$$

Remark 13. For $k > 1$ the equation $\lambda^2 = 1$ has only four solutions in $\mathbb{Z}_{2^{k+1}}$, but it must be observed that, for Propositions 6 and 7, the right solution is $\lambda = 2^k + 1$.

We now recall Nechaev's permutation [5] (see also [12]).

Definition 14. Let n be a positive odd integer and let τ be the permutation on $\{0, 1, \ldots, 2n-1\}$ given by

$$\tau = (1, n+1)(3, n+3)\cdots(2i+1, n+2i+1)\cdots(n-2, 2n-2).$$

The Nechaev permutation π on $\mathbb{F}_2^{2n}$ is defined as

$$\pi(a_0, a_1, \ldots, a_{2n-1}) = (a_{\tau(0)}, a_{\tau(1)}, \ldots, a_{\tau(2n-1)}).$$

For the main result of this section, the following extension of Nechaev's permutation will be useful.

Definition 15. Let n be a positive odd integer and for any positive integer s, the extension of Nechaev's permutation π_s on $(\mathbb{F}_2^{2n})^s$ is defined as

$$\pi_s(a^{(1)}|a^{(2)}|\ldots|a^{(s)}) = \pi(a^{(1)})|\pi(a^{(2)})|\ldots|\pi(a^{(s)}),$$

where $a^{(i)} \in \mathbb{F}_2^{2n}$.

For $k=1$, $\lambda=3 \in \mathbb{Z}_4$ and n an odd positive integer, the following relation (Proposition 3.7) is proved in [12].

$$\phi\tilde{\mu}_3 = \pi\phi.$$

As a consequence of Eq. (7), Definition 15 and the previous relation, we have

Proposition 16. *Let n be an odd positive integer and $\lambda = 2^k + 1 \in \mathbb{Z}_{2^{k+1}}$. Then*

$$\Phi\tilde{\mu}_\lambda = \pi_{2^{k-1}}\Phi. \tag{8}$$

Proof. Let $A \in \mathbb{Z}_{2^{k+1}}^n$, then

$$\begin{aligned}\Phi(\tilde{\mu}_\lambda(A)) &= (\phi\varphi_0^k(\tilde{\mu}_\lambda(A)), \phi\varphi_1^k(\tilde{\mu}_\lambda(A)), \ldots, \phi\varphi_{2^{k-1}-1}^k(\tilde{\mu}_\lambda(A)))\\ &= (\phi\tilde{\mu}_3\varphi_0^k(A), \phi\tilde{\mu}_3\varphi_1^k(A), \ldots, \phi\tilde{\mu}_3\varphi_{2^{k-1}-1}^k(A))\\ &= (\pi\phi\varphi_0^k(A), \pi\phi\varphi_1^k(A), \ldots, \pi\phi\varphi_{2^{k-1}-1}^k(A)) = \pi_{2^{k-1}}(\Phi(A)).\end{aligned}$$

□

The natural generalization of [12, Corollary 3.8] is the following:

Corollary 17. *Let n be an odd positive integer and for $k \geqslant 1$ let $\pi_{2^{k-1}}$ be the extension of Nechaev's permutation. If Γ is the generalized Gray image of a linear cyclic code over $\mathbb{Z}_{2^{k+1}}$, then $\pi_{2^{k-1}}(\Gamma)$ is a quasi-cyclic code.*

Proof. Derives immediately from Theorem 11, Proposition 12 and Eq. (8). □

5. Linear *hpo*-cyclic codes

In this section it will be useful to represent elements of $\mathbb{Z}_{2^{k+1}}^n$ as polynomials in the ring $\mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$. This is achieved via the polynomial representation map given by Eq. (1).

The operation "$\odot$" introduced in Section 2 can be extended to $\mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$ as follows: if $A(x)=\sum_{j=0}^{n-1} a_j x^j$ and $B(x)=\sum_{j=0}^{n-1} b_j x^j$ are elements of $\mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$ then

$$A(x)\odot B(x)=\sum_{j=0}^{n-1}(a_j\odot b_j)x^j. \tag{9}$$

In the same way, the action of the mappings φ_i^k is extended to $\mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$ as follows: if $A(x)=\sum_{j=0}^{n-1} a_j x^j \in \mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$ then

$$\varphi_i^k(A(x))=\sum_{j=0}^{n-1}\varphi_i^k(a_j)x^j, \quad i=0,1,\ldots,2^{k-1}-1 \tag{10}$$

and the action of the map φ^k on $\mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$ is

$$\varphi^k(A(x))=(\varphi_0^k(A(x)),\ldots,\varphi_{2^{k-1}-1}^k(A(x))).$$

Proposition 18. *Let $\lambda=2^k+1\in\mathbb{Z}_{2^{k+1}}$. Then a subset C of $\mathbb{Z}_{2^{k+1}}^n$ is a linear hpo-cyclic code of length n if and only if its polynomial representation is an ideal of the ring $\mathbb{Z}_{2^{k+1}}[x]/(x^n-\lambda)$.*

Proof. The proof is similar to the one given for linear cyclic codes over a finite field (see for example [8]). □

Proposition 19. *Let n be an odd positive integer and $\lambda=2^k+1\in\mathbb{Z}_{2^{k+1}}$. Then the map μ_λ from $\mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$ into $\mathbb{Z}_{2^{k+1}}[x]/(x^n-\lambda)$ given by*

$$\mu_\lambda(A(x))=A(\lambda x)$$

is a ring isomorphism.

Proof. The proof is similar to that given in [12] for the map μ in Proposition 2.3. □

An immediate consequence of the previous result is the following:

Corollary 20. *A subset I of $\mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$ is an ideal of $\mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$ if and only if $\mu_\lambda(I)$ is an ideal of $\mathbb{Z}_{2^{k+1}}[x]/(x^n-\lambda)$.*

Linear cyclic codes of length n over the ring $\mathbb{Z}_{p^{k+1}}$, where $p\geqslant 2$ is a prime and $(n,p)=1$, have been studied by several authors [2,7,10]. In particular it is shown that any cyclic code over $\mathbb{Z}_{p^{k+1}}$ can be thought of as an ideal in the ring $\mathbb{Z}_{p^{k+1}}[x]/(x^n-1)$ [7, Theorem 3.4], and that this is a principal ideal ring [7, Corollary 3.6]. It is also proved

that for any cyclic code, C, of length n over $\mathbb{Z}_{p^{k+1}}$, a collection of pairwise-coprime polynomials $F_0, F_1, \ldots, F_{k+1}$ (possibly equal to 1) in $\mathbb{Z}_{p^{k+1}}[x]$ of degree less than n exits such that $F_0F_1 \cdots F_{k+1} = x^n - 1$, and C is generated by the polynomial $G = \hat{F}_1 + p\hat{F}_2 + \cdots + p^k\hat{F}_{k+1}$, where $\hat{F}_i = (x^n - 1)/F_i$. In this situation $|C| = p^t$, where $t = \sum_{i=0}^{k}(k+1-i)deg(F_{i+1})$. Additionally, it is proved that the number of $\mathbb{Z}_{p^{k+1}}$-cyclic codes of length n is $(k+2)^r$, where r is the number of factors in a factorization of $x^n - 1$ as a product of basic irreducible pairwise-coprime polynomials [7].

For $p=2$, since $\mathbb{Z}_{2^{k+1}}[x]/(x^n-1)$ is a principal ideal ring and μ_λ is a ring isomorphism (Proposition 19), then $\mathbb{Z}_{2^{k+1}}[x]/(x^n - \lambda)$ is a principal ideal ring.

In order to illustrate the concepts introduced above, an example is provided. Let $n = 7$, $k = 2$ and $x^7 - 1 = (x - 1)(x^3 + x + 1)(x^3 + x^2 + 1)$ in $\mathbb{F}_2[x]$. By Hensel lifting over $\mathbb{Z}_8$ we find

$$x^7 - 1 = (x - 1)(x^3 + 6x^2 + 5x - 1)(x^3 + 3x^2 + 2x - 1).$$

Applying the ring isomorphism, μ_λ, with $\lambda = 5$, over $\mathbb{Z}_8$ we have

$$x^7 - 5 = (x - 5)(x^3 + 6x^2 + 5x + 3)(x^3 - x^2 + 2x + 3).$$

Let C be the *hpo*-cyclic code generated by the polynomial $G(x)=(x-5)(x^3+6x^2+5x+3)=x^4+x^3-x^2+2x+1$. Since this polynomial does not divide $2(G(x)\odot 2G(x))=4x^2$, then by Theorem 5, the images $\varphi^2(C)$ and $\Phi(C)$ are nonlinear. The minimum homogeneous weight of C is 10. Hence $\Phi(C)$ is a $(28, 512, 10)$-binary nonlinear quasi-cyclic code of order 2. Observe that the largest minimum distance for binary linear codes of length 28 and dimension 9 is 10 [1,9] whereas it is 8 for binary linear cyclic codes. [2]

6. A family of linear images of linear *hpo*-cyclic codes

In this section $(\mathbb{F}_2[x]/(x^n - 1))^m$ (respect. $(\mathbb{Z}_{2^{k+1}}[x]/(x^n - 1))^m$) will denote the set of m-tuples whose entries are polynomials in the ring $\mathbb{F}_2[x]/(x^n - 1)$ (respect. $\mathbb{Z}_{2^{k+1}}[x]/(x^n - 1)$). Observe that with this notation, the isometry φ^k can be thought of as a map from $\mathbb{Z}_{2^{k+1}}[x]/(x^n - 1)$ into $(\mathbb{Z}_4[x]/(x^n - 1))^{2^{k-1}}$. For any positive integer m, the action of the Kronecker product, "$\otimes$", is also extended as follows: if $\bar{a}(x) = (a_1(x), \ldots, a_m(x)) \in (\mathbb{F}_2[x]/(x^n - 1))^m$ and $b(x) \in \mathbb{F}_2[x]/(x^n - 1)$, then

$$\bar{a}(x) \otimes b(x) = (a_1(x)b(x), \ldots, a_m(x)b(x))$$

and equivalently for $\bar{A}(x) \otimes B(x)$ with $\bar{A}(x) \in (\mathbb{Z}_{2^{k+1}}[x]/(x^n - 1))^m$ and $B(x) \in \mathbb{Z}_{2^{k+1}}[x]/(x^n - 1)$.

As a consequence of the polynomial representation of $\mathbb{Z}_{2^{k+1}}^n$ and Proposition 4 we have the following:

[2] This largest minimum distance, for binary linear cyclic codes of length 28 and dimension 9, was obtained with the help of a computer.

Proposition 21. *Let* $\lambda = 2^k + 1$ *and* $A(x), B(x) \in \mathbb{Z}_{2^{k+1}}[x]/(x^n - \lambda)$, *where* $A(x) = \sum_{j=0}^{n-1} a_j x^j$, *then*

$$\varphi^k(2^k A(x) + B(x)) = \bar{1} \otimes 2\tilde{a}(x) + \varphi^k(B(x)),$$

where $\tilde{a}(x)$ *is the polynomial in* $\mathbb{F}_2[x]/(x^n - 1)$, *whose coefficient of the monomial of degree* j *is one if and only if* a_j *is odd, for* $j = 0, \ldots, n-1$. *The product* $2\tilde{a}(x)$ *is taken in* $\mathbb{Z}_4[x]/(x^n - 1)$.

The following result in [12] describes a family of $\mathbb{Z}_4$-linear negacyclic codes of length n whose Gray map images are binary linear cyclic codes of length $2n$.

Theorem 22. *Let* n *be an odd positive integer and let* $\tilde{a}(x), \tilde{b}(x)$ *be in* $\mathbb{F}_2[x]$ *such that* $x^n - 1 = (x-1)\tilde{a}(x)\tilde{b}(x)$, *where* $(x-1), \tilde{a}(x)$ *and* $\tilde{b}(x)$ *are pairwise coprime. Let* $a_1(x), b_1(x)$ *be the Hensel lifts of* $\tilde{a}(x)$ *and* $\tilde{b}(x)$ *to* $\mathbb{Z}_4[x]$, *respectively, and define* $a(x) = a_1(-x)$ *and* $b(x) = b_1(-x)$. *If* $\tilde{C}$ *is the binary linear cyclic code of length* $2n$ *generated by* $\tilde{g}(x) = \tilde{a}(x)^2\tilde{b}(x)$, *then* $\tilde{C}$ *is the Gray map image of the* $\mathbb{Z}_4$*-linear negacyclic code of length* n *generated by* $g(x) = a(x)(b(x) + 2)$. *Furthermore, if* $u(x) \in \mathbb{Z}_4[x]/(x^n + 1)$ *and* $\tilde{u}(x) \in \mathbb{F}_2[x]$ *are such that the coefficient of the monomial of degree* j *in* $\tilde{u}(x)$ *is one if and only if the coefficient of the monomial of degree* j *in* $u(x)$ *is an odd number, then*

$$\phi(u(x)g(x)) = [f(u(-1))\tilde{b}(x) \oplus \tilde{u}(x)(x+1)]\tilde{g}(x),$$

where f *is the function from* $\mathbb{Z}_4$ *into* $\mathbb{F}_2[x]$ *given by* $f(a) = \phi(a) \cdot (1, x)$, *where as usual "·" is the dot product.*

The function f in the previous theorem can be extended to $\mathbb{Z}_4^m$ as follows: if $A = (a_1, \ldots, a_m) \in \mathbb{Z}_4^m$, then $f(A) = (f(a_1), \ldots, f(a_m))$.

In analogy to the previous theorem, we are interested in a family of *hpo*-cyclic codes whose φ^k and Φ images are linear codes. Let $\tilde{a}(x)$ and $\tilde{b}(x)$ be as in Theorem 22 and let $A_1(x), B_1(x)$ and $C_1(x)$ be the Hensel lifts of $\tilde{a}(x)$, $\tilde{b}(x)$ and $(x-1)$ to $\mathbb{Z}_{2^{k+1}}[x]$, respectively. Since $A_1(x), B_1(x)$ and $C_1(x)$ are pairwise coprime polynomials, it can be proved that the ideal generated by $A_1(x)(B_1(x) + 2^k C_1(x))$ is also generated by $A_1(x)(B_1(x) + 2^k)$. In this way, one of those families of *hpo*-cyclic codes is obtained as the ideals whose generator polynomial has the form $A_1(\lambda x)(B_1(\lambda x) + 2^k)$. More precisely, we have

Theorem 23. *For* $k > 1$, *let* n *be an odd positive integer and using the previous notation, define* $A(x) = A_1(\lambda x)$ *and* $B(x) = B_1(\lambda x)$. *If* C *is the linear hpo-cyclic code generated by* $G(x) = A(x)(B(x) + 2^k)$, *then the image* $\varphi^k(C)$ *is a quaternary linear quasi-negacyclic code of order* 2^{k-1} *and length* $2^{k-1}n$. *Also,* $\Phi(C)$ *is a binary linear quasi-cyclic code of order* 2^{k-1} *and length* $2^k n$. *Furthermore, if* $U(x) \in \mathbb{Z}_{2^{k+1}}[x]/(x^n - \lambda)$ *and* $\tilde{u}(x) \in \mathbb{F}_2[x]$ *are such that the coefficient of the monomial of degree* j *in* $\tilde{u}(x)$ *is one if and only if the coefficient of the monomial of degree* j *in* $U(x)$ *is an odd*

number, then

$$\varphi^k(U(x)G(x)) = \varphi^k(U(\lambda)) \otimes [a(x)b(x)] + \bar{1} \otimes [2\tilde{u}(x)\tilde{a}(x)],$$

$$\Phi(U(x)G(x)) = [f(\varphi^k(U(\lambda))) \otimes \tilde{b}(x) \oplus \bar{1} \otimes (\tilde{u}(x)(x+1))] \otimes \tilde{g}(x). \tag{11}$$

Proof. The quasi-negacyclicity of the code $\varphi^k(C)$ follows from Theorem 8, and the quasi-cyclicity of $\Phi(C)$ follows from Theorem 11. It is easy to see that $2((u+2^k v)\odot w) = 2(u \odot w)$ and $2(v\lambda \odot w\lambda) = 2(v \odot w)\lambda$, for all $u, v, w \in \mathbb{Z}_{2^{k+1}}$. Now observe that for all $U(x)$, we have $U(x)A(x)B(x) = U(\lambda)\sum_{j=0}^{n-1} \lambda^j x^j$ in $\mathbb{Z}_{2^{k+1}}[x]/(x^n - \lambda)$. Thus it follows from Eq. (9) that $2((G(x)U_1(x)) \odot (G(x)U_2(x))) = G(x)(2(U_1(\lambda) \odot U_2(\lambda)))$, for all $U_1(x), U_2(x) \in \mathbb{Z}_{2^{k+1}}[x]/(x^n - \lambda)$, and the linearity of these codes follows from Theorem 5.

It follows from Proposition 21 that $\varphi^k(U(x)G(x)) = \varphi^k(U(x)A(x)B(x)) + \bar{1} \otimes [2\tilde{u}(x)\tilde{a}(x)]$, and Eqs. (4) and (10) show that, for all $i=0,\ldots,2^{k-1}-1$, $\varphi_i^k(U(x)A(x)B(x)) = \varphi_i^k(U(\lambda))\sum_{j=0}^{n-1}(-1)^j x^j = \varphi_i^k(U(\lambda))a(x)b(x)$, proving the first Eq. in (11).

Observe that for each i, $\varphi_i^k(U(\lambda))$ is an odd number if and only if $\tilde{u}(1)$ is also an odd number, and therefore $u_i(x) \in \mathbb{Z}_4[x]/(x^n+1)$ must exist such that $u_i(-1) = \varphi_i^k(U(\lambda))$ and the coefficient of the monomial of degree j in $u_i(x)$ is an odd number if and only if the coefficient of the monomial of degree j in $\tilde{u}(x)$ is one. Thus, each polynomial $\varphi_i^k(U(\lambda))a(x)b(x) + 2\tilde{u}(x)\tilde{a}(x)$ in the entries of $\varphi^k(U(x)G(x))$ can be rewritten as $u_i(x)g(x)$ in the ring $\mathbb{Z}_4[x]/(x^n+1)$. Applying Theorem 22 to those polynomials we get the final part of the proof. □

An example is given to illustrate the above result. Let $k=2$, $n=7$, $\lambda=5$ and $x^7-1 = (x-1)\tilde{a}(x)\tilde{b}(x)$, with $\tilde{a}(x) = x^3+x+1$ and $\tilde{b}(x) = x^3+x^2+1$, then

$$a(x) = 3x^3 + 2x^2 + 3x + 3,$$

$$b(x) = 3x^3 + 3x^2 + 2x + 3,$$

$$A(x) = 5x^3 + 6x^2 + x + 7,$$

$$B(x) = 5x^3 + 3x^2 + 2x + 7,$$

$$\tilde{g}(x) = x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1,$$

$$g(x) = x^6 + 3x^5 + x^4 + x^3 + x^2 + x + 3,$$

$$G(x) = x^6 + 5x^5 + x^4 + x^3 + x^2 + x + 5.$$

The generalized Gray map image of the *hpo*-cyclic code generated by the polynomial $G(x)$ is a $[28, 6, 12]$-binary linear quasi-cyclic code of order 2 given by the set

$$[\tilde{g}(x)\tilde{u}_1(x) \,|\, \tilde{g}(x)\tilde{u}_1(x) + ((x^{14}-1)/(x-1))\tilde{u}_2(x)]$$

for all $\tilde{u}_1(x), \tilde{u}_2(x) \in \mathbb{F}_2[x]$, where all polynomial multiplications are taken modulo $x^{14}-1$.

Acknowledgements

The authors would like to thank the two referees for their comments that improved the presentation of this paper. This work was partially done while the first author was on sabbatical at DGSCA, UNAM.

References

[1] A.E. Brouwer, Bounds on the size of linear codes, in: W.C. Huffman, V.S. Pless (Eds.), Handbook of Coding Theory, Vol. I, North-Holland, Amsterdam, The Netherlands, 1998, 295–461. See also updated tables at http://www.win.tue.nl/∼aeb/voorlincod.html.
[2] A.R. Calderbank, N.J.A. Sloane, Modular and p-adic cyclic codes, Design Codes and Cryptography 6 (1) (1995) 21–35.
[3] C. Carlet, $\mathbb{Z}_{2^k}$-linear codes, IEEE Trans. Inform. Theory 44 (1998) 1543–1547.
[4] M. Greferath, S.E. Schmidt, Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code, IEEE Trans. Inform. Theory 45 (1999) 2522–2524.
[5] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.
[6] W. Heise, T. Honold, A.A. Nechaev, Weighted modules and representations of codes, in: Proceedings ACCT 6, Pskov, Russia, 1998, 123–129.
[7] P. Kanwar, S.R. Lopez-Permounth, Cyclic codes over the integers modulo p^m, Finite Fields and Their Appl. 3 (4) (1997) 334–352.
[8] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland, Amsterdam, The Netherlands, 1977.
[9] P. Piret, Good linear codes of length 27 and 28, IEEE Trans. Inform. Theory 26 (1980) 227–230.
[10] V. Pless, Z. Qian, Cyclic codes and quadratic residue codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 42 (1996) 1594–1600.
[11] G. Vega, H. Tapia-Recillas, On $\mathbb{Z}_{2^k}$-linear and quaternary codes, submitted for publication (available from the authors).
[12] J. Wolfmann, Negacyclic and cyclic codes over $\mathbb{Z}_4$, IEEE Trans. Inform. Theory 45 (1999) 2527–2532.